AMENDMENT TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in this application:

Listing of Claims:

1. (Currently amended) A tracking system for use with an identification medium to provide time-limit access to a resource. comprising:

a transmitter module secured to the identification medium;

a receiver module in selective communication with the transmitter module;

the transmitter module including an encryptor and a time generator that generates a temporal sequence of values (T_{Bn}), wherein the encryptor encrypts the temporal sequence of values (T_{Bn}) with a private, non-public key K_n which is unique to the identification medium to generate a code list composed of encrypted code elements $(T_{Bn})K_n$, and wherein the transmitter module transmits one or more encrypted code elements $(T_{Bn})K_n$ to the receiver module; [[and]]

a server, connected to the receiver module, for storing the private key of the identification medium, and including an authenticator that authenticates one or more of the encrypted code elements of the code list; and

wherein the private key is available only to the server and to the identification medium, thus preventing an observer from identifying and tracking the identification medium.

2. (Original) The tracking system according to claim 1, for use with a plurality of identification media, each identification medium including a transmitter module and a unique private key for transmitting at least one or more of the encrypted code elements $(T_{Bn})K_n$ to the receiver module for authentication.

3. (Original) The tracking system according to claim 2, wherein the server stores private keys of the plurality of identification media.

4. (Original) The tracking system according to claim 3, wherein the receiver module provides unidirectional communication with at least one of the plurality of identification media.

5. (Original) The tracking system according to claim 3, wherein upon authenticating the identification medium, the authenticator provides authentication information to an application for initiating the application.

6. (Original) The tracking system according to claim 3, wherein the private key is represented by a bit-string having a length of at least 48 bits.

7. (Original) The tracking system according to claim 5, wherein the transmitter module transmits the encrypted code elements at a predetermined transmission cycle.

8. (Original) The tracking system according to claim 3, wherein the temporal sequence of values is measured from an initial synchronized starting point of each identification medium.

9. (Original) The tracking system according to claim 1, wherein the temporal sequence of values is incremented in equal time increments.

10. (Original) The tracking system according to claim 7, wherein the authenticator creates an authentication table composed of precalculated

encrypted code elements for every identification medium, and further attempts to match the encrypted code elements transmitted by the transmitter module to the precalculated encrypted code elements in the authentication table.

11. (Original) The tracking system according to claim 10, wherein the server encrypts the temporal sequence of values (T_{Bn}) and an offset time value (T_{on}) for each identification medium with a corresponding unique private key K_n to generate a list of authentication codes, En, as represented by the following expression:

$$En = (T_{Bn} + T_{on})_{Kn}.$$

12. (Original) The tracking system according to claim 11, wherein the temporal resolution of the authentication table exceeds the transmission cycle of the transmitter module.

13. (Original) The tracking system according to claim 12, wherein the temporal resolution of the authentication table is approximately 1 second; and wherein the transmission cycle is approximately 10 seconds.

14. (Original) The tracking system according to claim 11, wherein the transmitter module transmits at least one encrypted code element to the receiver module as a packet; and

wherein the packet includes three fields: a preamble field, a payload field, and a checksum field.

15. (Original) The tracking system according to claim 14, wherein the preamble field contains data bits indicating that the packet is originating from a valid identification medium;

the payload field contains an encrypted code element $(T_{Bn})K_n$; and wherein the checksum field allows for checking transmission integrity.

16. (Original) The tracking system according to claim 11, wherein the temporal sequence of values (T_{Bn}) is represented by the following expression;

$$(T_{Bn})=T_{system}-T_{n\ creation},$$

where T_{system} represents current time for the server, and $T_{n\ creation}$ represents a creation time of the identification medium referenced to a same time standard as T_{system};

and wherein the server stores $T_{n\ creation}$ for each identification medium.

17. (Original) The tracking system according to claim 16, wherein the server establishes a clock synchronization window for the list of authentication codes, En, to account for time drift between the current time of the identification medium and a current time of the server.

18. (Original) The tracking system according to claim 17, wherein the clock synchronization window is centered around the current time (T_{Bn}) of the identification medium, as shown by the following expressions:

$$En1 = (T_{Bn} + T_{on})_{Kn},$$

$$En2 = (T_{Bn} + T_{on} - \text{Epsilon})_{Kn}, \text{ and}$$

$$En3 = (T_{Bn} + T_{on} + \text{Epsilon})_{Kn},$$

wherein En1 is the authentication code when the identification medium is in general synchrony with the server;

wherein En2 is the authentication code when the identification medium lags the server; and

wherein En3 is the authentication code when the identification medium leads the server;

wherein Epilson is the resolution of the temporal sequence of values (T_{Bn})

19. (Original) The tracking system according to claim 1, wherein the transmitter module is incorporated in any one or more of: an identification badge, a card, or a label.

20. (Original) The tracking system according to claim 19, wherein the identification medium includes any one or more of: a credit card, a dining card; a telephone calling card; a health card; a driver's license; a video store card; a car access card; a computer access card; or a building access card; an identification tag, a key fob.

21. (Currently amended) A tracking method for use with a plurality of identification media to selectively provide time-limit access to a resource, comprising:

encrypting the temporal sequence of values (T_{Bn}) of the identification media with private, non-public keys K_n that are unique to each identification medium, to generate a transmission comprised of encrypted code elements $(T_{Bn})K_n$;

securely storing the private keys of the plurality of identification media; [[and]]

authenticating the transmitted encrypted code elements $(T_{Bn})K_n$ by creating an authentication table composed of precalculated encrypted code elements for the identification media for the temporal sequence of values (T_{Bn}), and further attempting to match encrypted code elements $(T_{Bn})K_n$ to the precalculated encrypted code elements in the authentication table; and

wherein the private key is available only to the server and to the identification medium, thus preventing an observer from identifying and tracking the identification medium.

22. (Original) The tracking method according to claim 21, wherein authenticating the encrypted code elements includes encrypting a temporal sequence of values (T_{Bn}) and an offset time value (T_{on}) for each identification medium with a corresponding unique private key K_n to generate a list of encrypted code elements, En, as represented by the following expression:

$$Fn = (T_{Bn} + T_{on})_{Kn}.$$

23. (Currently amended) A wireless identification system for use with an identification medium to provide access to a resource, comprising:

a sequence generator to generate a temporal sequence of values (TBn);

a private, non-public key Kn that is unique to the identification medium;

an encryptor to receive a temporal sequence value and the private key, and to output an encrypted result;

a transmitter module secured to the identification medium to receive the encrypted result and to output a wireless signal;

a receiver module to receive the wireless signal and output the encrypted result; [[and]]

an authenticator, to receive the encrypted result and the private key Kn, and to output an access authorization signal; and

wherein the private key is available only to the server and to the identification medium, thus preventing an observer from identifying and tracking the identification medium.

24. (Original) The wireless identification system according to claim 23, for use with a plurality of identification media, each identification medium including a

transmitter module and a unique private key for transmitting one or more of the encrypted results to the receiver module for authentication.

25. (Original) The wireless identification system according to claim 24, wherein the authenticator stores private keys of the plurality of identification media.

26. (Original) The wireless identification system according to claim 23, wherein the authenticator pre-calculates future encrypted results.

27. (Original) The wireless identification system according to claim 26 wherein the future encrypted results are distributed to a remote authenticator to enable time-limited access to a resource.

28. (Original) The wireless identification system according to claim 24, wherein the temporal sequence of values is measured from an initial synchronized starting point of each identification medium.

29. (Original) The wireless identification system according to claim 24, wherein the temporal sequence of values is incremented in equal time increments.

30. (Original) The wireless identification system according to claim 24, wherein the transmitter module outputs the wireless signal periodically.

31. (Original) The wireless identification system according to claim 24, wherein the transmitter module outputs the wireless signal upon external stimulus, wherein the external stimulus is any one or more of: a mechanical switch, a motion detector, a light detector, or a sound detector.

32. (Original) The wireless identification system according to claim 24, wherein the authenticator creates an authentication table composed of pre-calculated encrypted code elements for every identification medium, and further attempts to match the encrypted code elements transmitted by the transmitter module to the pre-calculated encrypted code elements in the authentication table.

33. (Original) The wireless identification system according to claim 24,wherein the temporal sequence of values (TBn) is represented by the following expression;

(TBn)=Tsystem-Tn creation,

where Tsystem represents current time for the authenticator, and Tn creation represents a creation time of the identification medium referenced to a same time standard as Tsystem; and

wherein the server stores Tn creation for each identification medium.

34. (Original) The wireless identification system according to claim 33, wherein the authenticator establishes a clock synchronization window for the list of authentication codes, En, to account for time drift between the current time of the identification medium and a current time of the authenticator.

35. (Original) The wireless identification system according to claim 34, wherein the clock synchronization window is centered around the current time (TBn) of the identification medium, as shown by the following expressions:

En1 = (TBn + Ton)Kn,

En2 = (TBn + Ton Epsilon)Kn, and

En3 = (TBn + Ton + Epsilon)Kn,

where En1 is an authentication code when the identification medium is in general synchrony with the server;

where En2 is an authentication code when the identification medium lags the server;

where En3 is an authentication code when the identification medium leads the server; and

where Epilson is an resolution of the temporal sequence of values (TBn).

36. (Original) The wireless identification system according to claim 24, wherein the transmitter module is incorporated in any one or more of: an identification badge, a card, or a label.

37. (Original) The wireless identification system according to claim 36, wherein the identification medium includes any one or more of: a credit card, a dining card; a telephone calling card; a health card; a driver's license; a video store card; a car access card; a computer access card; or a building access card; an identification tag, a key fob.

38. (Original) The wireless identification system according to claim 25, wherein upon authenticating the identification medium, the authenticator provides authentication information to an application for initiating the application.

39. (Original) The wireless identification system according to claim 24, wherein the authenticator encrypts the temporal sequence of values (TBn) and an offset time value (Ton) for each identification medium with a corresponding unique private key Kn to generate a list of authentication codes, En, as represented by the following expression:

$$En = (TBn + Ton)Kn.$$